The SSE-CMM & Evaluations: Partners within the Assurance Framework

Charles G. Menk III

V21, DoD

menk@romulus.ncsc.mil

Overview

- Introduction
- The Assurance Framework
- Vision and goals of SSE CMM
- Evaluation Concerns
- SSE CMM Solutions
- Recommendations
- Summary

Motivation

- Increased use of commercial products
- Commercial development cycles shorter than evaluation time lines
- Move from risk avoidance to risk management

Areas of Focus

- Qualification
  - How to believe someone is capable of doing the job
- Specification
  - What criteria can be used as a basis for an adequate measurement of capability
- Verification
  - Proof that the job is done correctly

The Assurance Framework

- Comprehensive integration of assurance
  - Trusted Capability Maturity Model (TCMM)
  - System Security Engineering CMM (SSE CMM)
  - ISO 9000
  - X/Open Branding
  - Testing
  - Evaluation

Statistics on CMM for Software ROI

Measure	Range	Median
Cost of SPI per engineer	$490-2004	$1475
Annual productivity gain	9%-67%	35%
Defects discoverd pre-test	6%-25%	22%
Reduction in post-release defects	10%-94%	39%
Value returned on each dollar invested	4-8	5

Source: Benefits of CMM-Based Software Process Improvement, SEI, August 1994

System Security Engineering CMM

- Apply CMM concepts to Security Engineering
- Process improvement mechanism
- Capability-based measurement of Security Engineering process
- Developed “stand-alone” extension of the SEI System Engineering Methods

SSE CMM: A Community Effort

- Driven by industry-led Working Groups
- Facilitated by NSA
- Office of Secretary of Defense supplemented NSA funding
- Volunteers for pilot assessments in mid-1996
- Seeking commercial home for model
- Internet Web Site: http://www.ssecmm.ashton.csc.com

Vision Statement

- To provide secure solutions NOW
- To provide the most assurance at the least cost:
  - In Time & Money
    - To the DoD and its Partners
  - Return On Investment
    - Security within the bounds of budget
    - CMM to target “after-market” cost reduction
      - Risk avoidance (patch and play) to risk management
- To do it with grace

Goal and Objective

- To have security built-in from day one
- To KNOW it is being done right
- To assist in educating developers, those called upon to analyze the products and systems, and their customers

The SSE CMM Process Areas

- Specify Security Needs
- Provide Security Input
- Verify and Validate Security
- Penetrate Security

The SSE CMM Process Areas (cont.)

- Assess Security Risk
- Assure Security
- Monitor System Security Posture
- Manage System Security Controls
- Coordinate Security

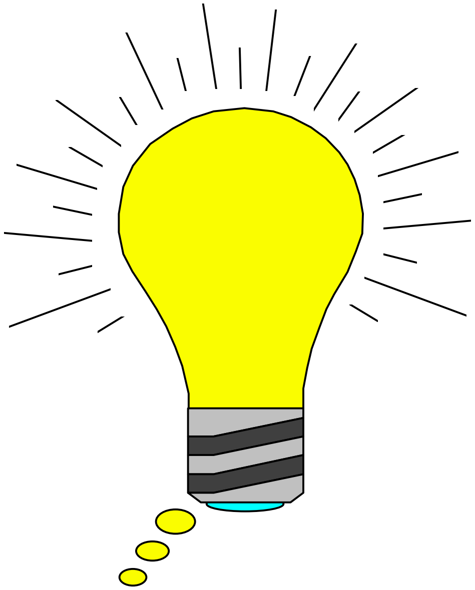
Evaluation Concerns

- Documentation
  - Does not reflect implementation
  - Not detailed enough
- Code
  - Not verifiable
  - Undocumented
  - Flaws

How Did We Get Here?

- Add-on Security
- Reduced Development Time Lines
- Systems too large and complex
- Evaluators expected to do too much
  - Educate about security
  - Assist in design modifications
  - Assist in documentation development

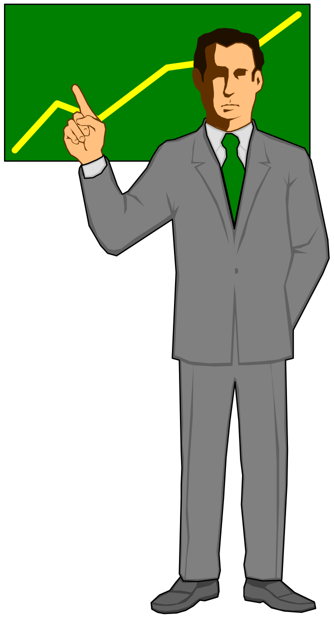
SSE-CMM Solutions



- Address security from day one
- Create confidence in developer abilities
  - Documentation
  - Configuration Management
  - Error detection and correction
  - Continuous improvement

Current Status of SSE-CMM

- Draft 1.0 now available
- Pilots completed in June-October 1996
  - Combined assessments
  - Stand alone assessments
  - Add-on assessments
  - Special case assessments



Pilot Results to Date

Let Them Eat Cake

- Bakeries should be able to bake cakes
- Certain bakers are better than others
- Some bakers have baked cakes
- Some use a recipe
- So how do you pick a good cake?
  - Taste it when done (Evaluate)
  - Pick a professional cake baker (CMM)

Recommendation

- Guide SSE CMM development to provide output that has diverse utility
  - Evaluations
  - Accreditation & Certification
  - Profiles
- Use SSE CMM to gain assurance that the developer CAN build secure products
- Potential support to RAMP process NOW

For Additional Information

- John Adams
  - Chief, V213 Process Engineering
- Trusted Capability Maturity Model
  - Amy Mastranadi
- System Security Engineering CMM
  - Chuck Menk

(410) 859-6091